THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **PAIGE THOMPSON'S RESPONSE TO THE GOVERNMENT'S MOTION TO SEAL AND REDACT ADMITTED TRIAL EXHIBITS**

I. INTRODUCTION

Paige Thompson, through counsel, opposed in part the government's motion to seal and redact admitted trial exhibits. The Court should protect the public's right to view the code in Exhibits 204-205, 252, 461, 608, 640, 644-647, 670, 674-677, and 803-804 because the government's concern that "others could copy [the code]" falls drastically short of a "compelling reason" to overcome the "strong presumption of public access."[1] (Dkt. 355 at 2; LCR 5(g).) Ms. Thompson does not object to sealing Exhibits 506 and 731, nor does Ms. Thompson object to redacting personal identifying information like account numbers and PII consistent with the local rules. That said, the defense does object to the government's characterizations of what occurred at trial.

[1] Exhibit 461 is a slight exception because it is an excerpt of an Internet Relay Chat (IRC) containing code and some statements.

II. FACTUAL BACKGROUND

On June 23, 2022, the government offered a proposal to certify admitted exhibits. On June 24, 2022, the defense agreed to the proposal. On June 27, 2022, prior to filing the certification, the government requested an agreement from the defense to seal certain exhibits in their entirety and partially redact other exhibits. Specifically, the government requested that Exhibits 204-205, 252, 608, 640, 644-647, 670, 674-677, 731, and 803-804 be sealed in their entirety. The government further requested that Exhibits 201-202, 455, 461, 506, 642, 643, 802, 806-812, 901-904, 914-922, and 956 be redacted in part. The defense opposed for a number of reasons, including the fact that some did not comply with the local rules. *See* Local Criminal Rules 49.1, 55(b) and (c); *see* Local Civil Rule 5(g).[2] Having met and conferred, the government filed a motion seeking to redact in its entirety or partially the same exhibits except Exhibits 201-202, and 642, which the government no longer seeks to have redacted.

III. ARGUMENT

The Court should not seal Exhibits 204-205, 252, 461, 608, 640, 644-647, and 803-804. The defense does not object to redacting personal identifying information consistent with the local rules, like account numbers, as an alternative to sealing those exhibits.

In its motion, the government offered no basis to suggest there is a "substantial probability" that another person will copy Ms. Thompson's code or that "there are no alternatives to [sealing] that would adequately protect" companies who utilize AWS servers. *United States v. Doe*, 870 F.3d 991, 998 (9th Cir. 2017); *see Hagestaf v. Tragesser*, 49 F.3d 1430, 1434 (9th Cir. 1995) ("[T]he district court must base its

[2] Local Civil Rule 5(g)(3)(B) incorporates the applicable standard to the sealing of documents under circuit precedent. *See United States v. Doe*, 870 F.3d 991, 998 (9th Cir. 2017). The rule is directly referenced in Local Criminal Rule 55(c).

decision on a compelling reason . . . without relying on hypothesis or conjecture.") Additionally, the remedy of sealing otherwise publicly-accessible documents would not prevent future instances of hacking because the code Ms. Thompson utilized here has been widely disseminated (and dissected) within the tech community. *See, e.g.,* E. Covert, *Case Study: AWS and Capital One*, System Weakness (Aug. 28, 2021), *available at* https://systemweakness.com/case-study-aws-and-capital-one-c4ad6cb71c79 (last visited August 2, 2022); R. Wright, *Capital One hack highlights SSRF concerns for AWS*, TechTarget (Aug. 5, 2019), *available at* https://www.techtarget.com/searchsecurity/news/252467901/Capital-One-hack-highlights-SSRF-concerns-for-AWS (last visited Aug. 2, 2022). Additionally, AWS publicly discloses much of the same scripting that Ms. Thompson utilized on its own security blog and user guides. *See, e.g.,* C. MacCarthaigh, *Add defense in depth against open firewalls, reverse proxies, and SSRF vulnerabilities with enhancements to the EC2 Instance Metadata Service*, AWS Security Blog (Nov. 19, 2019), *available at* https://aws.amazon.com/blogs/security/defense-in-depth-open-firewalls-reverse-proxies-ssrf-vulnerabilities-ec2-instance-metadata-service/ (last visited Aug. 2, 2022); *IAM roles for Amazon EC2*, AWS User Guide for Linux Instances, *available at* https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/iam-roles-for-amazon-ec2.html (last visited August 2, 2022). The cat is already out of the proverbial bag and has been so for going on three years, which weighs strongly in favor of allowing public access to these documents.

The government's fear that bad-faith hackers will copy Ms. Thompson's code is misplaced for a number of reasons. (*See* Gov't Mot. at 3-4.) The usability of that code is also focused on IAM roles, a feature found only on AWS servers, and AWS already reached out to and notified its customers with similar firewall configurations to address the possibility of so-called "copycat attackers." (6/8/22 Tr. at 116.) Further, this incident attracted widespread media attention, so the "word is out." There is no "substantial probability that, in the absence of [sealing]," the government's concern will materialize. (Dkt. 355 at 2-3 (quoting *Doe*, 870 F.3d at 998).)

Moreover, before this case, "[e]ach individual step [of her process] was relatively well-known." (6/8/22 Tr. at 117.) Although "the ability to combine these steps . . . was not widely known" at the time, Ms. Thompson sparked rich discussions and efforts in Internet security circles to change the settings for firewalls and overly permissive roles that allowed her code to succeed. (*Id.*; *see also* 6/13/22 Tr. at 86 (explaining at trial that 42Lines limited Ms. Thompson's permissions within its servers by implementing the principle of least privilege).)

Lastly, disclosing Ms. Thompson's code would add clarity to Computer Fraud and Abuse Act ("CFAA") case law, which continues to perplex Internet security researchers. As the Court has noted, "there has long been concern among the security researcher community about how their actions may be criminal under the CFAA." (Dkt. 226 at 10.) And recent decisions by the Supreme Court and the Ninth Circuit likely made security researchers even less certain as to what behavior might trigger CFAA liability. *See Van Buren v. United States*, 141 S. Ct. 1648, 1658 (2021) (describing the CFAA's authorization requirement as a "gates-up-or-down inquiry"); *hiQ Labs*, *Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1197 (9th Cir. 2022) (finding that the CFAA does not apply to publicly available information, even where the computer system operator specifically bans and actively attempts to thwart scraping of that information). These decisions led this Court to acknowledge that Ms. Thompson's code "exists in a gray area" that requires the "interstitial work of . . . hard line-drawing." *See* Dkt. 226 at 8 & n.5 (quoting Orin Kerr, *Focusing the CFAA in* Van Buren, SUP. CT. REV. (forthcoming)). Given this case likely represented the first time any court has drawn such a line since the Ninth Circuit's decision in *hiQ*, *see* Dkt. 330 at 20-24 (instructing the jury on *hiQ*'s language), security researchers would surely find immense value in inspecting Ms. Thompson's code to discern where liability might attach to their day-to-day work.

IV. CONCLUSION

For the foregoing reasons, Ms. Thompson respectfully requests the Court deny, in part, the government's motion.

DATED: August 4, 2022

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson